(12) UK Patent Application (19) GB (11) 2 248 324 (13) A

(43) Date of A publication 01.04.1992

(21) Application No 9020896.8

(22) Date of filing 25.09.1990

(51) INT CL[5]
G06F 12/14 1/00

(52) UK CL (Edition K)
G4A AAP

(56) Documents cited
GB 2228350 A EP 0008355 A1 US 4734855 A

(58) Field of search
UK CL (Edition K) G4A AAP
INT CL[5] G06F 1/00 12/14
Online database: WPI

(71) Applicant
Uken (Research & Development) Limited

(Incorporated in Ireland)

Gortnafluir, Clonmel, County Tipperary, Ireland

(72) Inventors
Joseph Flynn
Shemas Elvers

(74) Agent and/or Address for Service
Marks & Clerk
57-60 Lincoln's Inn Fields, London, WC2A 3LS, United Kingdom

(54) Data security in a computer network

(57) A microcomputer 1 is disclosed which is adapted for connecting in a computer network where there is shared access to stored data. The microcomputer comprises a security circuit 5 which controls operation of an address buffer 6 according to a table of access conditions retrieved from non-volatile memory in response to an input password, there being one access condition for each block of memory addresses. Passwords have assigned security levels and a respective table of access conditions for each level is held in the non-volatile memory. The relevant memory address block is identified by reading of a memory map that has been created and stored by the security circuit 5 in the non-volatile memory. The microcomputer thus assists in preventing accidental amendment of data, fraud by amendment of financial data, and access to confidential data.

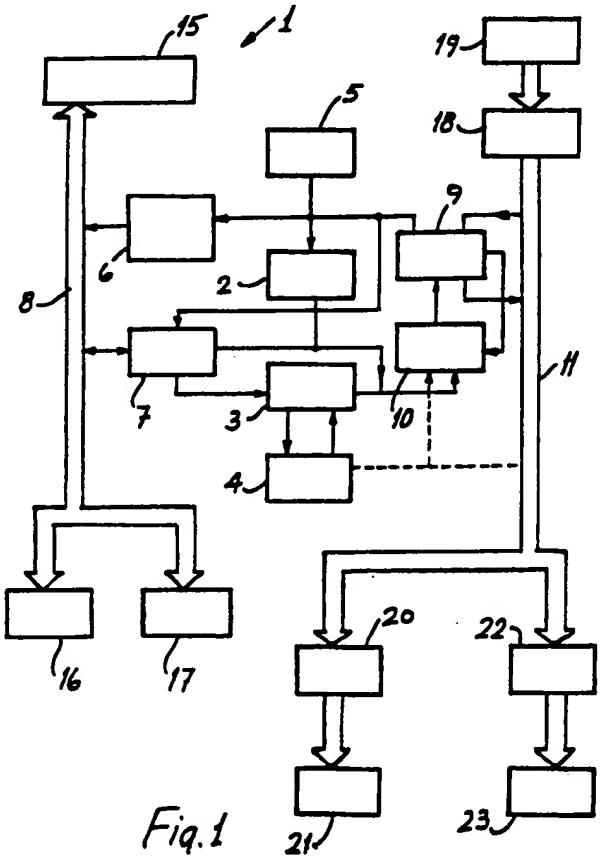

Fig.1

GB 2 248 324 A

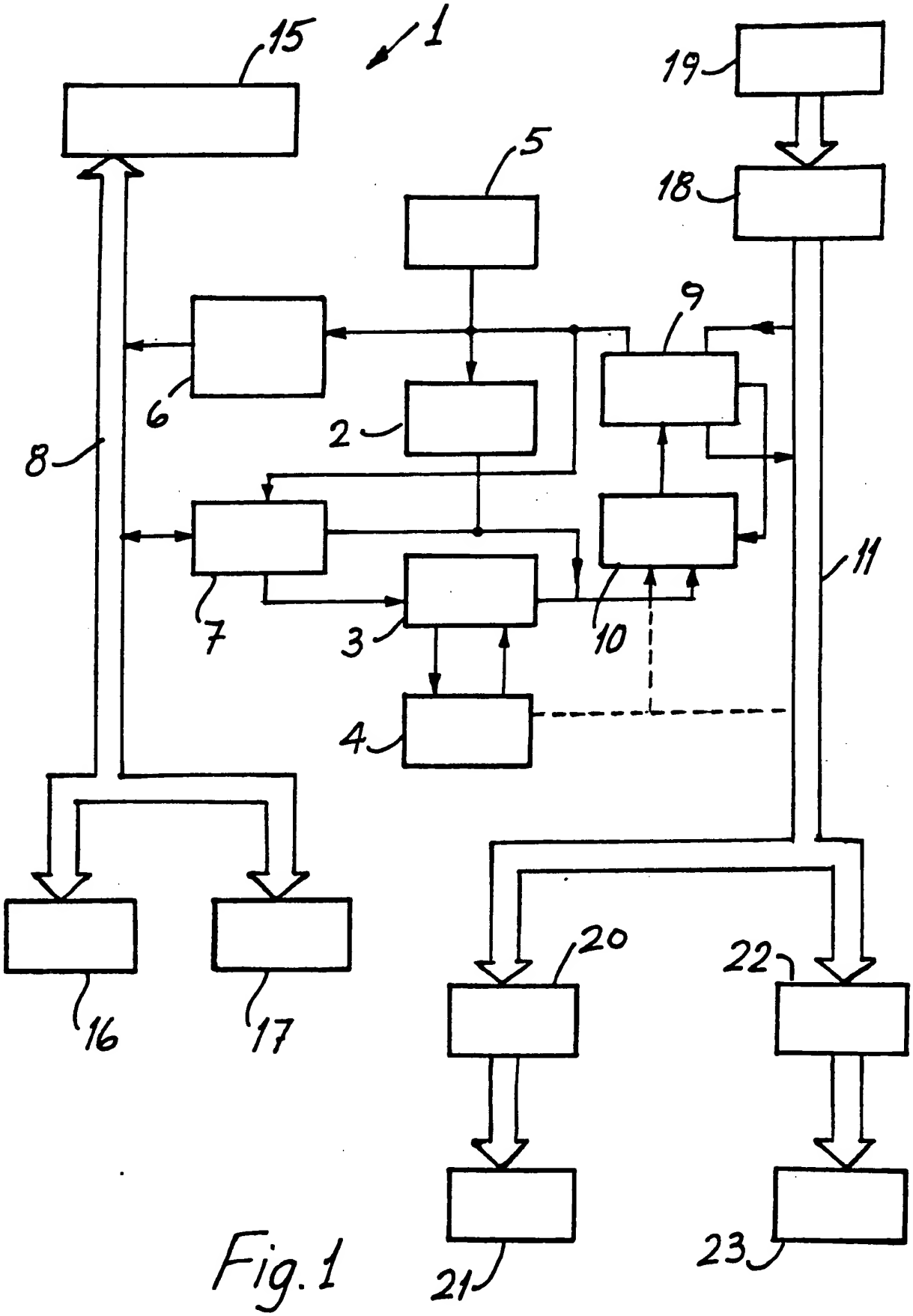

Fig. 1

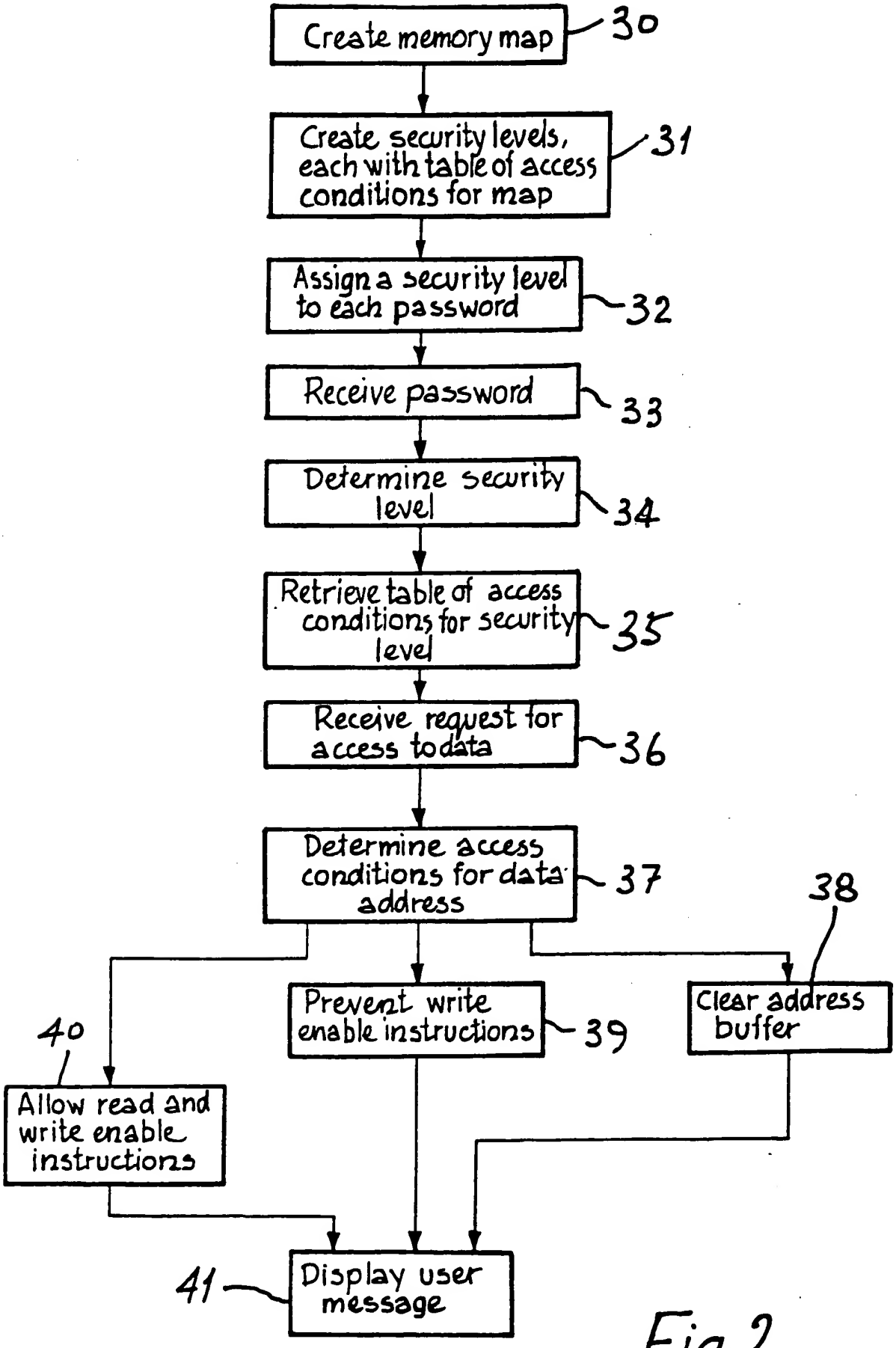
Create memory map
30
Create security levels, each with table of access conditions for map
31
Assign a security level to each password
32
Receive password
33
Determine security level
34
Retrieve table of access conditions for security level
35
Receive request for access to data
36
Determine access conditions for data address
37
38
40
Prevent write enable instructions
39
Clear address buffer
Allow read and write enable instructions
41
Display user message

Fig. 2

0-15 Kb	16-31 Kb	32-47 Kb	48-63 Kb
1	3	2	2
64-79 Kb	80-95 Kb	96-111 Kb	112-127 Kb
3	3	3	1
128-143 Kb	144-159 Kb	160-175 Kb	176-191 Kb
1	2	3	1

Fig. 3

"Security in a Computer Apparatus"

The present invention relates to security in a computer apparatus, and more particularly to security of stored data in a network computer apparatus.

Control of access to stored data to prevent loss of confidentiality of the data, fraud involving financial data, accidental loss or amendment of the data or deliberate falsification of data has been achieved with some success for stand-alone computers. However, where there is shared access to stored data in a computer network, such control has not been achieved without excessively limiting the manner in which users may use the network and introducing time delays in operation. This is particularly true where the network may be accessed by a remote computer. Indeed, in some cases the manner in which access is controlled in these situations in many instances renders a computer network useless. For example, where interlinked by communications links, and each is used to monitor manufacturing or project activities on-site, programs for controlling access to data can require excessively large memory areas, and generate excessive communications traffic and introduce unnecessary restrictions

to the extent that the networks fail to perform their most important functions which is to provide up-to-date information when and where it is required.

The present invention is directed towards solving these problems.

According to the invention, there is provided a microcomputer adapted to be connected in a network for shared access to stored data and to allow access to the stored data in a controlled manner to maintain confidentiality of data, avoid fraud and accidental loss or amendment of data, the microcomputer comprising:-

a control unit having a security circuit; an arithmetic unit; and a memory transfer unit;

a memory bus connecting the memory transfer unit to a random access memory, and to a non-volatile memory including a fixed disk and a shared memory device via a network interface;

an input/output bus connecting the arithmetic unit to a keyboard encoder, to a video controller and to a printer controller connected respectively to a keyboard, a visual display unit and a printer;

wherein the security circuit comprises means for directing storage in the non-volatile memory of security data comprising a plurality of user passwords, a security level for each password, and a table comprising access conditions for each block of a memory map, there being one table for each security level, and wherein the security circuit comprises means for automatically retrieving relevant security data for storage in the random access memory circuit, for assigning a security level to a received password and for interactively controlling operation of the memory transfer circuit according to the access conditions when requests are received at the keyboard for access to data.

Ideally, there are three possible access conditions, namely, read and write disable, read enable and write disable and read and write enable.

In one embodiment, the security circuit interactively controls operation of the memory transfer circuit by control of memory instructions stored in an address buffer of the memory transfer circuit.

The invention will be more clearly understood when the following description of some preferred embodiments thereof, given by way of example only with reference to the accompanying drawings in which:-

Fig 1 is a block diagram of a microcomputer of the invention adapted for connecting in a computer network;

Fig 2 is a flow diagram illustrating operation of the microcomputer; and

Fig 3 is an illustration of portion of a sample security table generated in the microcomputer.

Referring to the drawings, and initially to Fig 1 there is illustrated a microcomputer of the invention indicated generally by the reference numeral 1. The microcomputer 1 is adapted to be connected in a computer network where there is shared access to data stored in a common memory device in the network. The microcomputer 1 comprises a control unit including a program counter 2, an instruction register 3 and a control and decode circuit 4. A security circuit 5 is also connected in the control unit. The control unit is connected to a memory transfer unit including an address buffer 6 and a data buffer 7, both of which are connected to a memory bus 8. An arithmetic unit comprising an accumulator 9 and an adder 10 is disposed between the control unit and an input/output bus 11. The memory bus 8 is connected to a random access memory circuit 15, to a fixed disk drive 16 and to a network interface 17. The input/output bus 11 receives inputs from the keyboard encoder 18 connected to a keyboard 19 and

provides outputs to a video controller 20 for a visual display unit (VDU) 21 and a printer controller 22 for a printer 23.

In operation, the microcomputer 1 is connected via the network interface 17 in a computer network where there is shared access to a common memory device. Such a computer network would be arranged to carry out many different types of data processing operations according to stored data and programs in the shared memory device. Each microcomputer would also have data and programs stored in the fixed disk 16. Referring specifically to Figs 2 and 3, operation of the microcomputer 1 to control access to data is illustrated.

Initially, the security circuit 5 directs storage in non-volatile memory which may be either the fixed disk 17 or the common memory device accessed via the network interface 17, of a memory map of 16 Kbyte blocks of addresses of stored data. Further, the security circuit 5 directs storage in non-volatile memory of a table made up of access conditions for each block of the memory map. Portion of such a table is shown in Fig 3. In this embodiment, there are five tables stored, one for each of five security levels identified by the numerals A, B, C, D and E. Security level A allows most access to data whereas security level E allows least access. Each table indicates one of three possible access conditions for each block of the memory map.

In Fig 2, the step of creating a memory map is indicated by the numeral 30 and of creating security levels and tables of access conditions by the numeral 31. In step 32, each password which is received from a supervisor who has full access to the data is assigned a security level according to the supervisor's instructions. The security circuit 5 directs storage of the password and of the security level in non-volatile memory. When a user wishes to have data processing operations carried out on the computer network, a password is received at the keyboard 19 in step 33 and in step 34, the security circuit retrieves the password for storage in the random access memory circuit 15 and determines the relevant security level A, B, C, D or E. The relevant table of access conditions for the security level is retrieved in step 35. When a request is received for access to data in step 36, the security circuit 5 determines access conditions for data which would be addressed in step 37. For each block of 16 Kbytes of data there is an access condition in the relevant table and the three possible access conditions are as follows:-

1. Read, write disable.

2. Read enable and write disable.

3. Read and write enable.

The first access condition applies where a user should not be allowed access to data to either view or amend the data. An example of such a situation is where a user who works in the purchasing department of an organisation is to be prevented from viewing the salary fields of a personnel system. The second access condition is suitable where a user is allowed to view the data such as purchasing prices, material delivery dates, without being allowed to amend the data. In these situations only certain specified users have the authority to amend data. It will be appreciated, for example, that if any unauthorised person amends data such as the purchasing price of an item, subsequent data processing operations carried out using that data would be useless. If the fact that there is a discrepancy is noticed, it would take a long time to find where the discrepancy arose and if it is not noticed the situation is even worse because wrong information is generated by the computer network. The third access condition is where a user such as a supervisor is allowed full access to data to both view it and to amend it, if required. For security level A, the table is made up fully of this access condition so that a supervisor may create new passwords and assign a security level and have full access to all of the data. This access condition may also be used selectively for different memory blocks according to the work which is carried out by each individual user. A portion of a sample table is shown in Fig 3. This table includes mixed access conditions for different memory blocks and is used for security level C.

For the memory address of the data which a user wishes to access, the security circuit 5 determines which block of the memory map the address falls within and retrieves from the table, the relevant access condition. If the access condition is number 1 above, the address buffer of the memory transfer unit is cleared by the security circuit 5 to prevent both write and read instructions being transmitted on the memory bus 8. If the access condition is number 2 above, the security circuit 5 prevents write enable instructions with step 39. If the access condition is number 2 above, the security circuit 5 allows both read and write enable instructions in the address buffer 6.

It will be appreciated that by use of microcomputers of the invention in a computer network, control of access to stored data will be achieved in a relatively simple and inexpensive manner. This is very important for large organisations where many different types of data are stored and it is important to avoid fraud by amendment of financial data, to avoid data errors caused by inadvertent write instructions and to prevent access to confidential data.

These operations are carried out in a sample manner by access to tables at each microcomputer in a network. In general it is preferable that the non-volatile memory used by the security circuit be the hard disk as this avoids the need for

accesses to the common memory device in the network. However, where network traffic is not a problem, the common memory device may be used.

The invention is not limited to the embodiments here and before described, but may be varied in construction and detail.

CLAIMS

A microcomputer adapted to be connected in a network for shared access to stored data and to allow access to the stored data in a controlled manner to maintain confidentiality of data, avoid fraud and accidental loss or amendment of data, the microcomputer comprising:-

a control unit having a security circuit; an arithmetic unit; and a memory transfer unit;

a memory bus connecting the memory transfer unit to a random access memory, and to a non-volatile memory including a fixed disk and a shared memory device via a network interface;

an input/output bus connecting the arithmetic unit to a keyboard encoder, to a video controller and to a printer controller connected respectively to a keyboard, a visual display unit and a printer;

wherein the security circuit comprises means for directing storage in the non-volatile memory of security data comprising a plurality of user passwords, a security level for each password, and a table comprising access conditions for each block of a memory map, there being one table for each security level, and wherein the

security circuit comprises means for automatically retrieving relevant security data for storage in the random access memory circuit, for assigning a security level to a received password and for interactively controlling operation of the memory transfer circuit according to the access conditions when requests are received at the keyboard for access to data.

2. A microcomputer is claimed in claim 1, wherein there are three possible access conditions, namely, read and write disable, read enable and write disable and read and write enable.

3. A microcomputer is claimed in claims 1 or 2, wherein the security circuit interactively controls operation of the memory transfer circuit by control of memory instructions stored in an address buffer of the memory transfer circuit.

4. A microcomputer substantially as hereinbefore described, with reference to and as illustrated in the accompanying drawings.

Patents Act 1977
Examiner's report to the Comptroller under Section 17 (The Search Report)

Application number
9020896.8

Relevant Technical fields

(i) UK Cl (Edition K) G4A (AAP)

(ii) Int Cl (Edition 5) G06F (1/00, 12/14)

Search Examiner
B G WESTERN

Databases (see over)

(i) UK Patent Office

(ii) Online database: WPI

Date of Search
6 November 1990

Documents considered relevant following a search in respect of claims

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
A	EP-0008355-A1 Siemens (whole document)	1-4
A	GB-2228350-A GSF (whole document)	1-4
A	US-4734855-A Banatre et al (whole document)	1-4

Category	Identity of document and relevant passages	Relevant to claim(s

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases